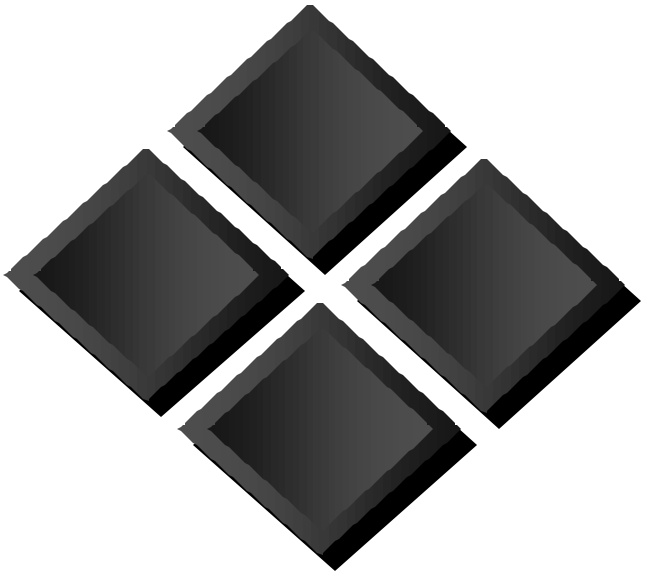


The Current State of National and International Standards for the Software Engineering of Mission Critical Systems

Paul R. Croll
Chair, IEEE SESC
Vice Chair ISO/IEC JTC1/SC7 US TAG
Computer Sciences Corporation
pcroll@csc.com

Mission Critical Systems Defined

- Can and must be trusted to work dependably to meet some mission critical requirement
- Failure to do so may have catastrophic results, such as serious injury, loss of life or property, mission failure, or breach of security
- Examples include:
  - weapons systems
  - avionics systems
  - command and control systems
  - intelligence systems
  - communications systems

[Source: NIST92]

Prerequisites for the Software Engineering of Mission Critical Systems

- Software engineering practices can either contribute to or detract from the integrity of a system
- To build high integrity software for mission critical systems, developers, assurers, and customers need an appropriately defined **body of knowledge**
  - for many engineering disciplines, such a body of knowledge may be found in handbooks and **rigorous standards**
  - such standards should give guidance on engineering practices that contribute to high integrity

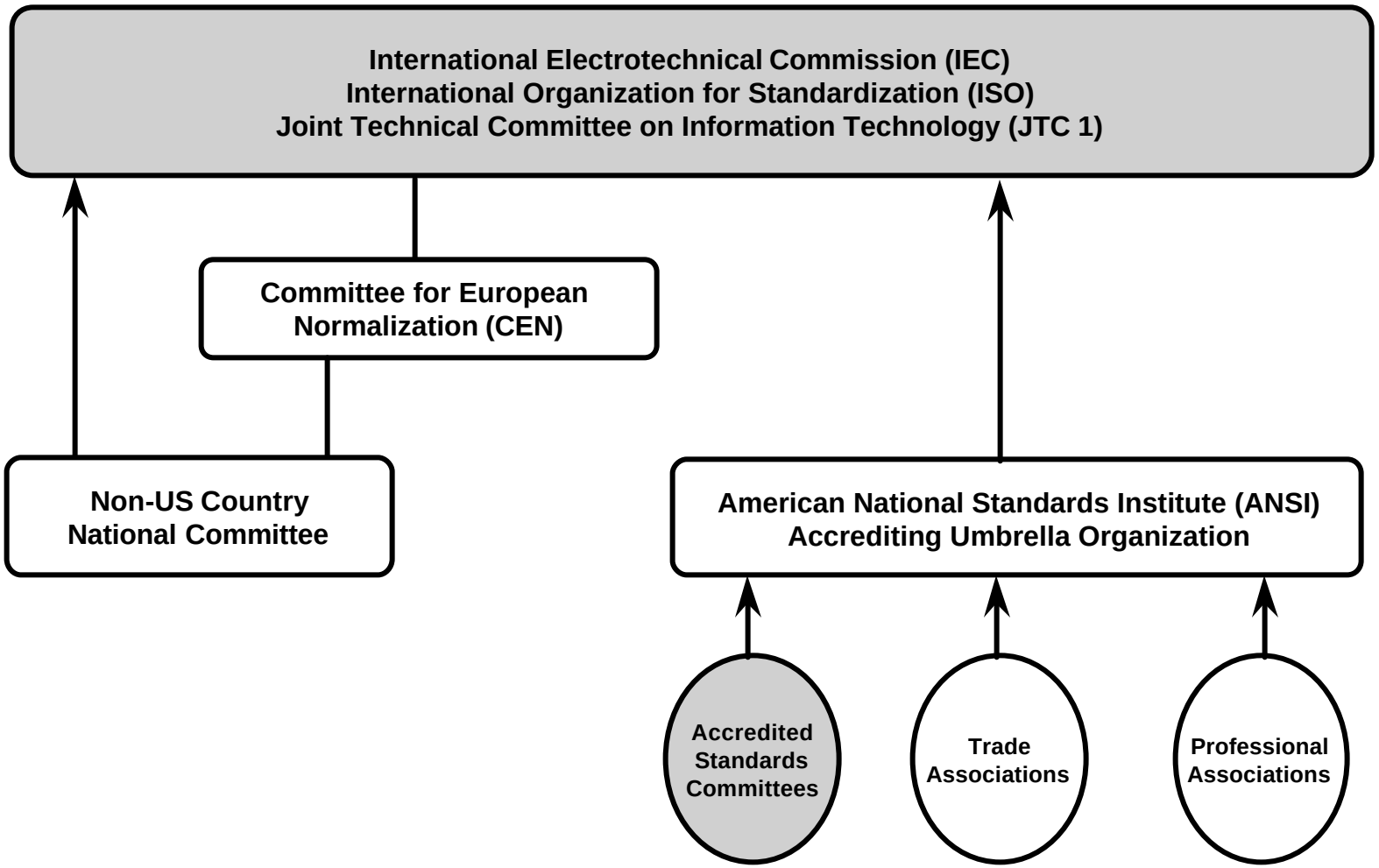
[Source: NIST92]

Discipline Through Process Standardization

- Software engineering process standards, are consensus-based standards that codify acceptable common practice
- This Code of Practice
  - consolidates existing technology into a firm basis for introducing newer technology
  - increases professional discipline
  - protects the business
  - protects the buyer
  - improves the product

[Source: Moore97]

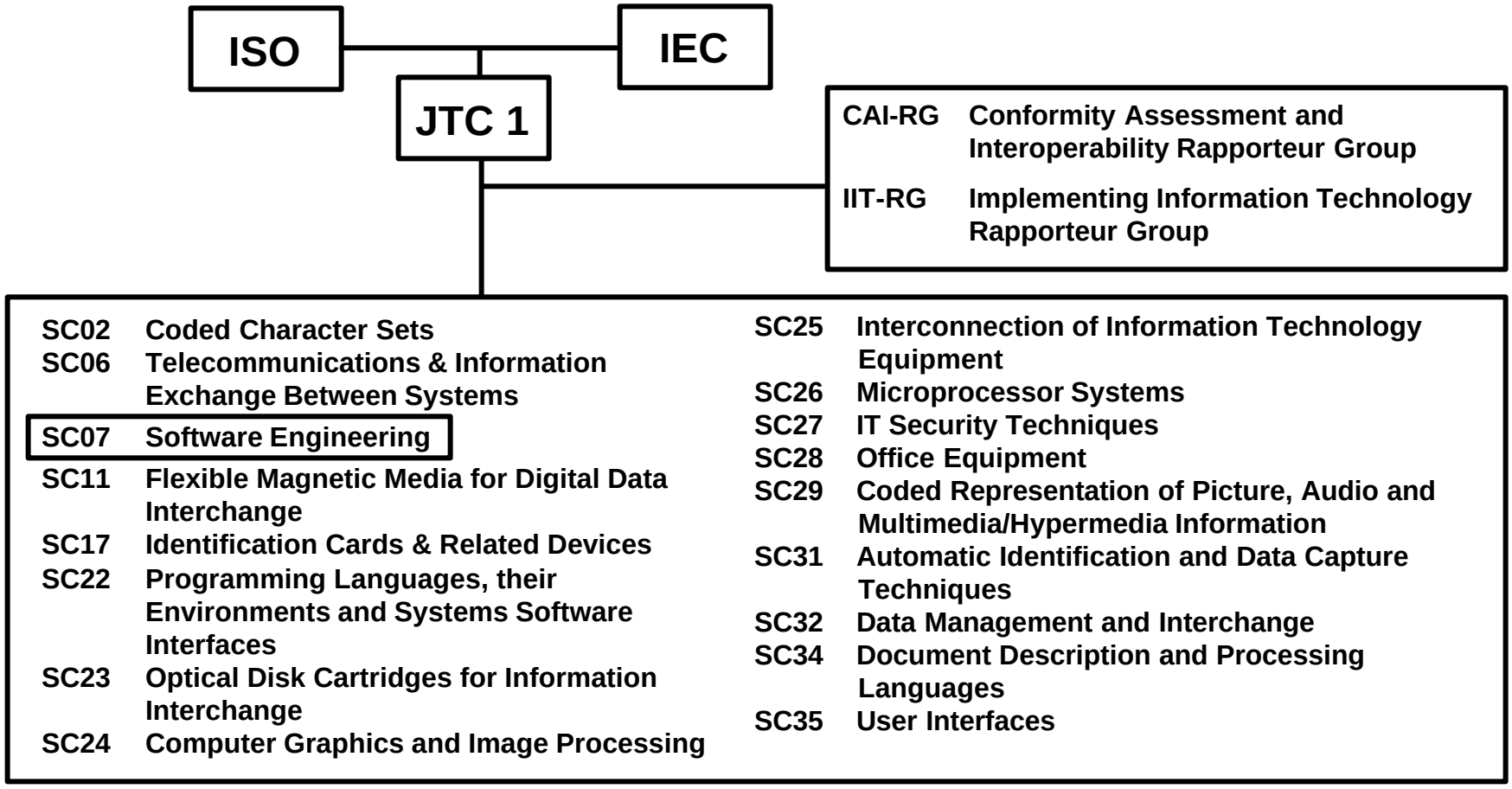
Context for Software Engineering Standards



ISO/IEC JTC1/SC7: Software Engineering

http://saturne.info.uqam.ca/Labo_Recherche/Lrgl/sc7/

ISO/IEC JTC1 Organization



ISO/IEC JTC1/SC7 Working Groups

- WG2: System software documentation
- WG4: Tools and environment
- WG6: Evaluation & metrics
- **WG7: Life cycle management**
- **WG9: System & SW integrity**
- **WG10: Process assessment**
- WG11: Software data definition and representation
- WG12: Functional size measurement
- **WG13: Software measurement process**
- SWG1: Planning
- SWG2: Vocabulary
- SWG3: Process Architecture
- Ad Hoc: Quality Mgmt
- Study Group: Risk Mgmt
- Study Group: Dependability and Reliability
- Study Group: SE Practices

■ = Mission Critical Systems Related

Current SC7 Standards

- **ISO/IEC 9126:1991, Product quality characteristics**
- ISO 9127:1988, User documentation and cover information for consumer software packages
- ISO/IEC TR 9294:1990, Management of software documentation
- ISO/IEC 11411:1995, Representation of state transition diagrams
- ISO/IEC 12119:1994, Software packages: Quality requirements and testing
- ISO/IEC TR 12182:1998, Categorization of software
- **ISO/IEC 12207:1995, Software life cycle processes**
- ISO/IEC 14102:1995, Evaluation and selection of CASE tools
- ISO/IEC 14143-1:1998, Functional size measurement
- ISO/IEC TR 14471:1999 Information technology -- Software engineering -- Guidelines for the adoption of CASE tools

■ = Mission Critical Systems Related

Current SC7 Standards - 2

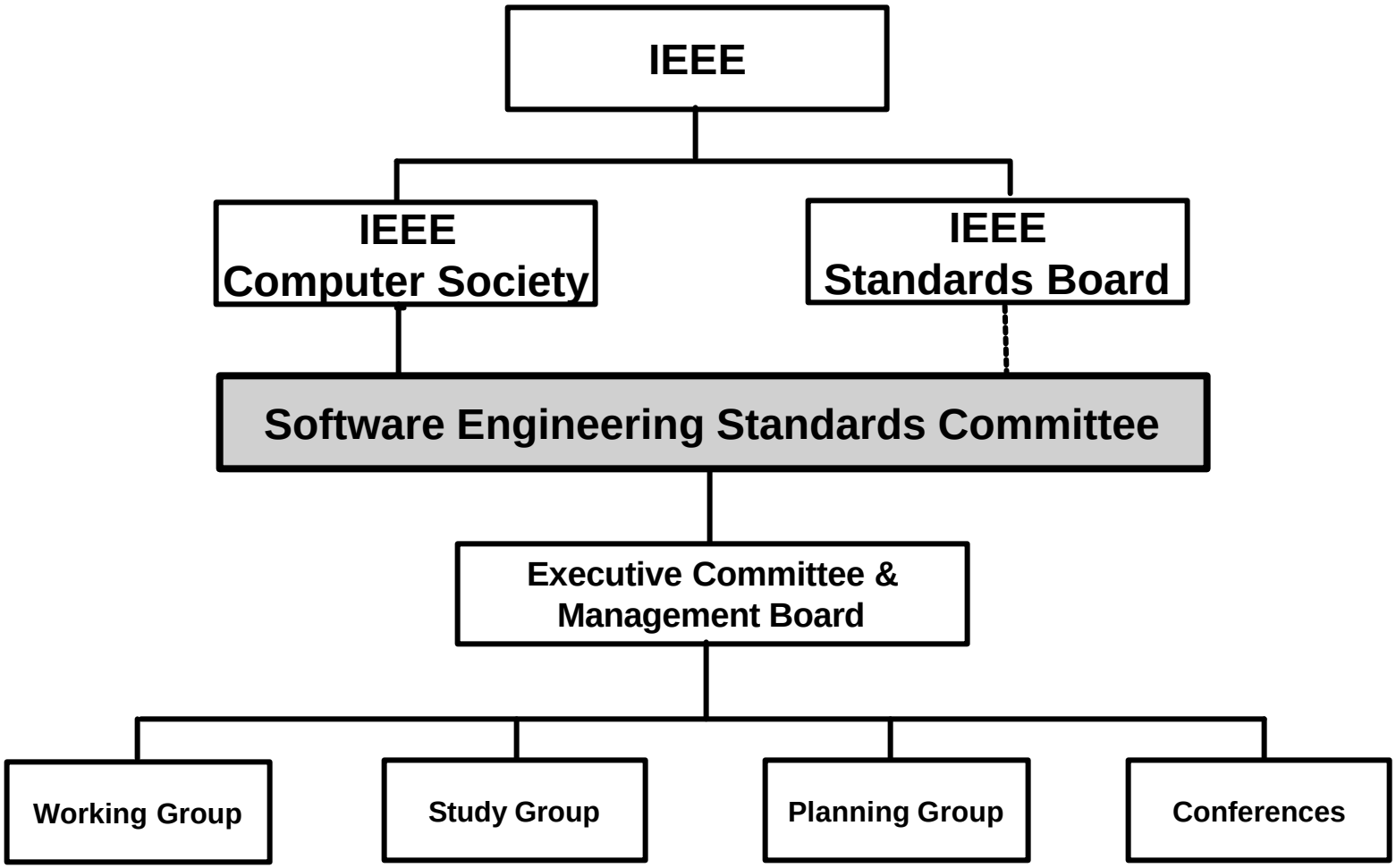
- ISO/IEC 14568:1997, Diagram exchange language for tree charts
- **ISO/IEC 14598:xxxx, Software product evaluation (3 of 6 parts)**
- ISO/IEC 14756:1999, Measurement and rating of performance
- ISO/IEC TR 14759:1999, Mockup and prototype
- ISO/IEC 14764:1999, Software maintenance
- **ISO/IEC 15026:1998, System and software integrity levels**
- ISO/IEC TR 15271:1998, Guide for ISO/IEC 12207
- **ISO/IEC TR 15504:1998, Software process assessment (9 parts)**
- ISO/IEC TR 15846:1998, SWLC processes - Configuration management
- ISO/IEC 15910:1999, Software user documentation process
- **Draft ISO/IEC 15939, Software Measurement Process**
- ISO/IEC TR 16326:1999, Software project management

■ = Mission Critical Systems Related

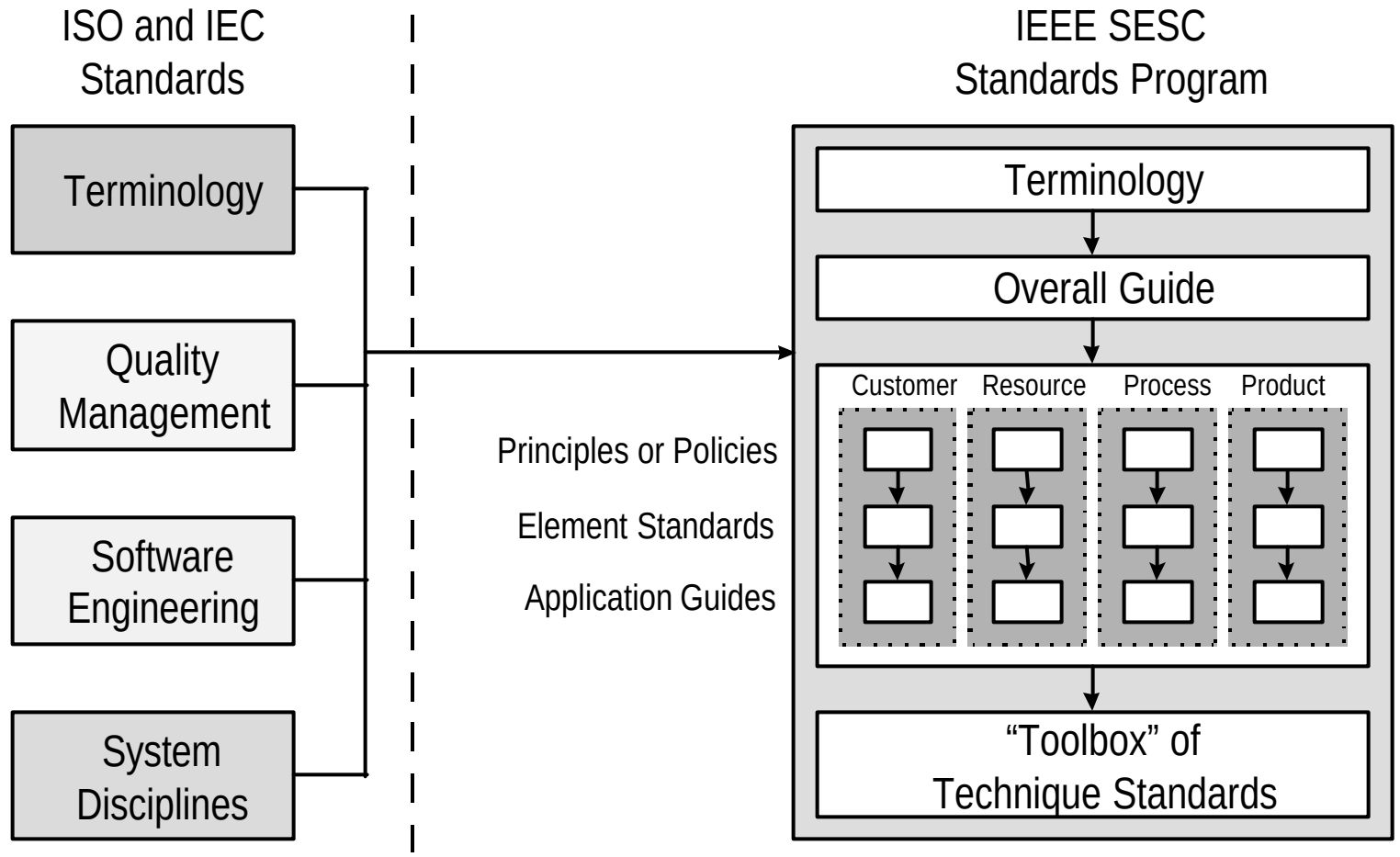
The IEEE Software Engineering Standards Committee (SESC)

http://computer.org/standard/sesc/

SESC in the IEEE Structure



SESC Strategic Program Model



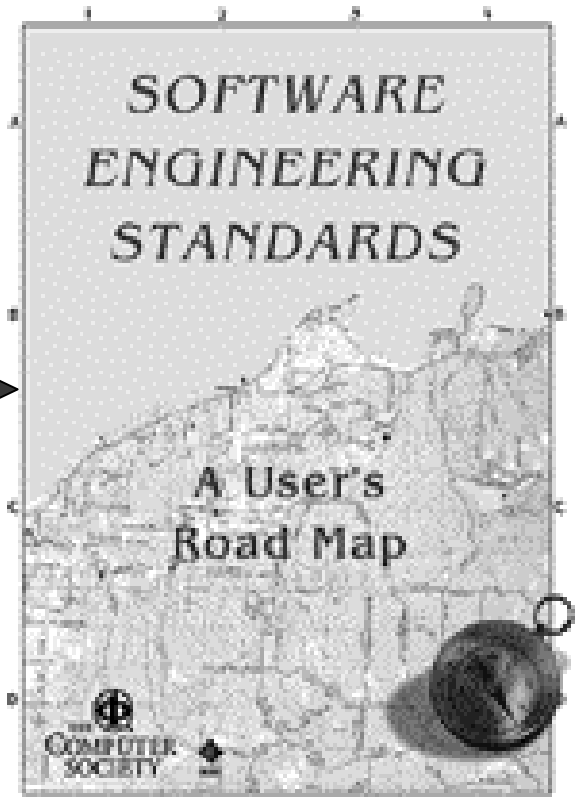
Source: [SESC95]

The IEEE Software Engineering Standards Collection

http://standards.ieee.org/catalog/softwareset.html

The 2000 Software Engineering Standards Collection

- Forty-six Standards
  - Customer & Terminology
  - Process
  - Product
  - Resource & Technique
- Overall guide
  - Several "views"
    - Context
    - Object
    - Normative intent
    - Provider and subject
  - Relationships among standards

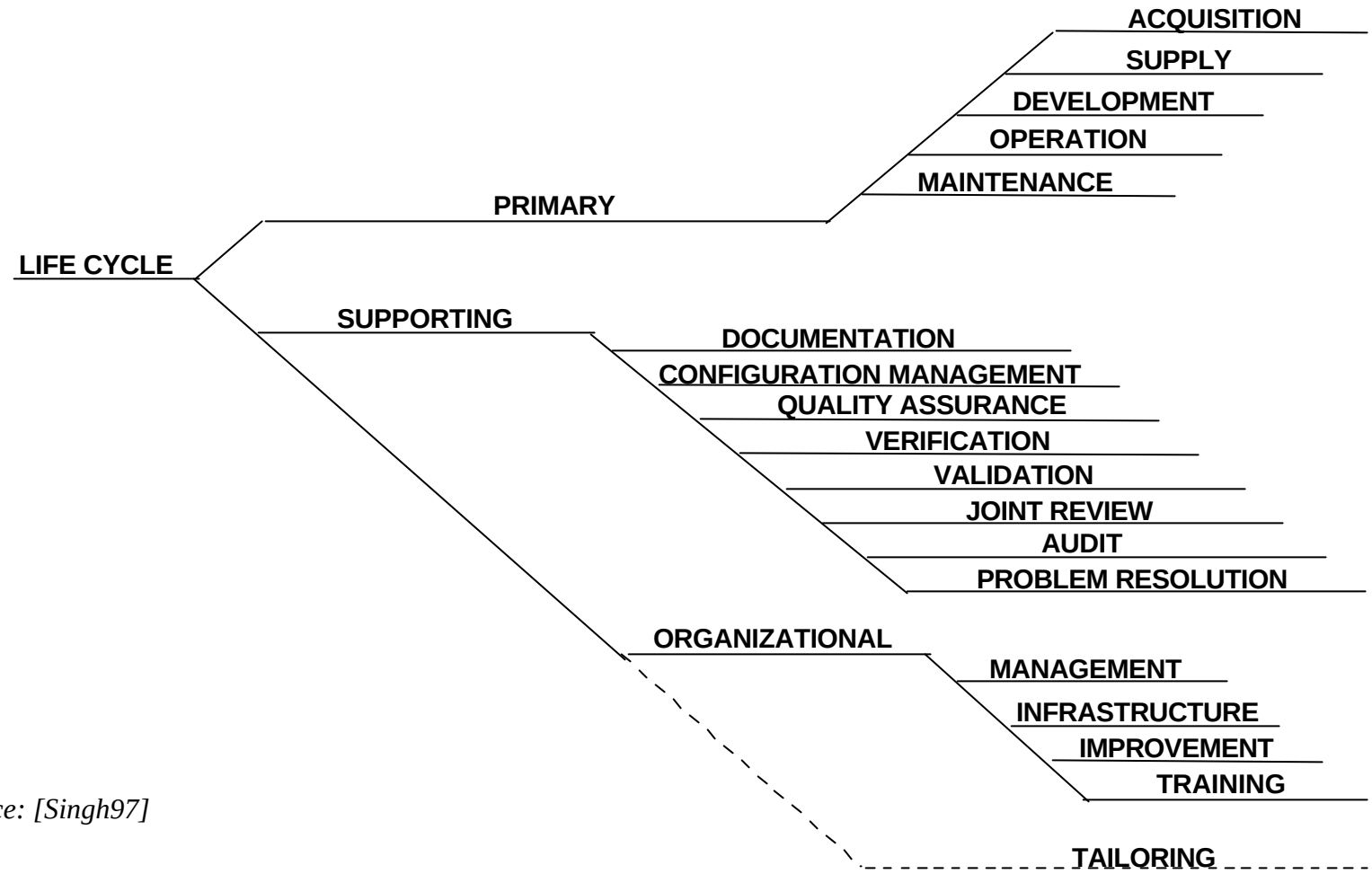


Source: [Moore97]

IEEE/EIA 12207: The Life Cycle Process Framework

- IEEE/EIA 12207, Standard for Information Technology – Software Life Cycle Processes
  - Addresses the complete software engineering life cycle, from acquisition and supply, through development, to operations and maintenance
  - Provides a process framework upon which an organization can build its enterprise-level life cycle processes
  - These enterprise-level processes are then tailored into projects, in order to meet specific project-level requirements.

IEEE/EIA 12207 Process Tree



Source: [Singh97]

Supporting Standards for Mission Critical Software

- IEEE/EIA 12207 relies upon other standards to fill in the details regarding the activities supporting life cycle processes.
- In the case of mission critical software, several additional software engineering standards are of interest.

Customer and Terminology

- 610.12, Standard Glossary of Software Engineering Terminology
- **1062, Recommended Practice for Software Acquisition**
- **1220, Standard for Application and Management of the Systems Engineering Process**
- **1228, Standard for Software Safety Plans**
- **1233, Guide for Developing System Requirements Specifications**
- **1362, Guide for Concept of Operations Document**
- **12207, Software Life Cycle Processes**
- **12207.1, Guide to Software Life Cycle Processes—Life Cycle Data**
- **12207.2, Guide to Software Life Cycle Processes—Implementation Considerations**

■ = Mission Critical Systems Related

Process

- 730, Standard for Software Quality Assurance Plans
- 730.1, Guide for Software Quality Assurance Planning
- 828, Standard for Software Configuration Management Plans
- **1008, Standard for Software Unit Testing**
- **1012, Standard for Software Verification and Validation**
- **1012a, Software Verification and Validation Content Map to IEEE/EIA 12207.1**
- 1028, Standard for Software Reviews
- 1042, Guide to Software Configuration Management
- 1045, Standard for Software Productivity Metrics
- 1058, Standard for Software Project Management Plans
- 1059, Guide for Software Verification and Validation Plans
- 1074, Standard for Developing Software Life Cycle Processes
- 1219, Standard for Software Maintenance
- 1490, A Guide to the Program Management Body of Knowledge

■ = Mission Critical Systems Related

Process - 2

- J-STD-016-1995, (EIA/IEEE) Interim Standard for Information Technology - Software Life Cycle Processes - Software Development - Acquirer-Supplier Agreement
- 1517-1999, Standard for Information Technology - Software Life Cycle Processes - Reuse Processes
- **P1540, D7.0, Draft Standard for Software Life Cycle Processes - Risk Management**

■ = Mission Critical Systems Related

Product

- **982.1, Standard Dictionary of Measures to Produce Reliable Software**
- **982.2, Guide for the Use of Standard Dictionary of Measures to Produce Reliable Software**
- 1061, Standard for a Software Quality Metrics Methodology
- 1063, Standard for Software User Documentation
- 1465, IEEE Standard Adoption of ISO/IEC 12119: 1994 (E) International Standard--Information Technology - Software Packages - Quality Requirements and Testing
- 14143.1, Approved Draft - Standard Adoption of ISO/IEC 1443-1:1998 - Information Technology - Software Measurement - Functional Size Measurement - Part 1: Definition of Concepts

■ = Mission Critical Systems Related

Resource and Technique

- **829, Standard for Software Test Documentation**
- **830, Recommended Practice for Software Requirements Specifications**
- **1016, Recommended Practice for Software Design Descriptions**
- 1044, Standard Classification for Software Anomalies
- 1044.1, Guide to Classification for Software Anomalies
- 1320.1, Syntax and Semantics for IDEF0
- 1320.2, Syntax and Semantics for IDEF1X97 (IDEFObject)
- 1348, Recommended Practice for the Adoption of CASE Tool
- 1420.1, Software Reuse—Data Model for Reuse Library Interoperability: Basic Interoperability Data Model
- 1420.1a, Software Reuse—Data Model for Reuse Library Interoperability: Asset Certification Framework
- 1420.1b-1999, Trial Use Supplement - Software Reuse—Data Model for Reuse Library Interoperability: Data Model for Reuse Library Interoperability: Intellectual Property Rights Framework

■ = Mission Critical Systems Related

Resource and Technique - 2

- 1430, Guide for Software Reuse - Concept of Operations for Interoperating Reuse Libraries
- 1462, Guide for the Evaluation and Selection of CASE Tools
- **P1471, Recommended Practice For Architectural Description of Software Intensive Systems**

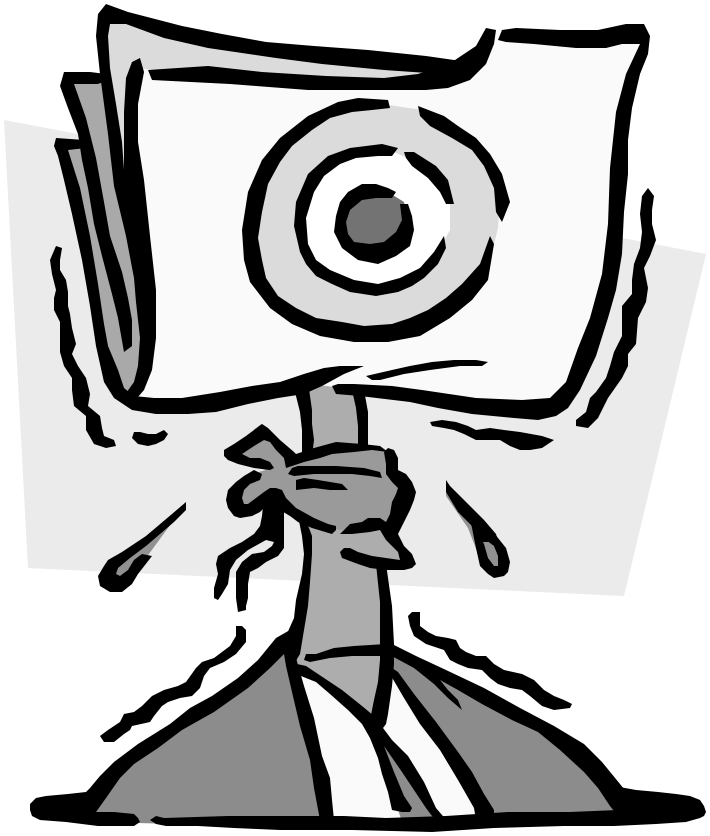
■ = Mission Critical Systems Related

How You Can Participate

- Join the IEEE Computer Society

  (at **http://www.computer.org**)
- Join the IEEE Software Engineering Standards Committee (at **http://www.tcse.org**)
  - Lead or participate in Working Groups developing or revising Standards
  - Lead or participate in Study Groups investigating new areas for standardization
  - Participate in SESC special projects
  - Become part of the SESC balloting pool (IEEE Standards Association membership required)

Questions



For more information . . .

Paul R. Croll
Computer Sciences Corporation
5166 Potomac Drive
King George, VA 22485-5824

Phone: +1 540.663.9251
Fax: +1 540.663.0276
e-mail: pcroll@csc.com

References

[Moore97] James W. Moore, *Software Engineering Standards: A User's Road Map*, IEEE Computer Society Press, Los Alamitos, CA, 1997.

[NIST92] NIST Special Publication 500-204, "High Integrity Software Standards and Guidelines," U.S. Dept. of Commerce, National Institutes of Standards and Technology, September 1992.

[SESC95] SESC Business Planning Group, "Vision 2000 Strategy Statement (Final Draft)," v0.9, SESC/BPG-002, August 20, 1995.

[Singh97] Raghu Singh, *An Introduction to International Standards ISO/IEC 12207, Software Life Cycle Processes*, 1997.